UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Criminal No. 18-20579

v.

Hon. Victoria A. Roberts

D-1 BRADLEY A. STETKIW,

Defendant.

**GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTION TO SUPRESS EVIDENCE OBTAINED OUTSIDE THE SCOPE OF THE SEARCH WARANT (Doc. 20)**

The United States of America opposes defendant Bradley A. Stetkiw's ("STETKIW's") motion to suppress evidence discovered in plain view during a computer search.

STETKIW maintains that a computer forensic examiner, in the course of a search authorized by warrant, had no authority to view a file that contained an image of child pornography. STETWKW argues that the examiner's review went beyond the scope of the warrant, and therefore that this image—and thereby images obtained through two subsequent warrants—must be suppressed.

STETKIW is wrong. The terms of the original warrant authorized the search of the target computer for content that could be—indeed, would likely be—

contained within image files. The examiner, therefore had the authority to review the file in question to determine its contents. And upon realizing its contents, the examiner followed standard procedure and the governing case law by stopping the search immediately so that a follow-up, expanded warrant could be obtained.

## FACTS

Supported by its accompanying affidavit, the warrant in question authorized a search of electronic devices for evidence of Operating an Unlicensed Money Transmitting Business in violation of 18 U.S.C. 1960. Exhibit 1. As recounted by the affidavit, this business was conducted through the exchange of bitcoins, a digital currency. Id.

The warrant specifically authorized the search of STEKIEW's electronic media. Attachment B of Exhibit 1. See also Affidavit of Exhibit 1 at p. 20 ¶ 15. The affidavit attested to three concepts relevant to the discovery of the instant photograph. First, that the storage and transfer of digital currency such as bitcoins requires the use of so-called digital "wallets." Affidavit of Exhibit 1 at pp 13-14 ¶ 19. These wallets are represented as a sequence of letters and numbers, up to 34 characters. Id. In order to access a wallet, it is necessary to have control of a private key, possibly a series of random words. Id. As the affidavit explains, bitcoin owners take various measures to ensure both access to, and the privacy of, this key. Id. Second, that the search of a computer is a lengthy, technical and exacting process

that requires the use of specialized software and various machine-assisted methods. Id. at pp 20-28 ¶¶ 14-19. Finally, forensic review of a computer is not solely about seeking evidence of a crime, but seeking attribution evidence that links a specific individual to that particular computer (and thereby the crimes under investigation). Affidavit of Exhibit 1 at 23-24 ¶ 17 b. The affidavit specifically notes that such attribution evidence can include images. Id.

Attachment B of the warrant reflects these concepts. For example, it authorized the seizure of cryptographic keys "in any form" used to access digital currency, and goes on to authorize the seizure of "private keys, wallet recover seeds, usernames, passwords, [and] mnemonic pins". Attachment B of Exhibit 1 at ¶¶ 1 b and 1 d. It specifically authorized the search for and seizure of attribution evidence—including photographs. Id. at ¶ 5 a.

The Government also proffers that, were the forensic examiner to testify, that he would swear to the following additional facts:

(1) In his training and experience, holders of digital currency commonly store their cryptographic keys and wallet addresses as image files;

(2) He was aware that the warrant permitted him to search electronic devices for evidence of attribution and identity, including photographs;

(3) That the forensic program used for his review of electronic devices "carves" images for review from all locations of a given device (including deleted items found in "slack space") and presents this images in a unified, continuous display of "thumbnail images";

(4) That during review of these "thumbnail images" he identified the image in question as depicting a child engaged in a sexual act; and

(5) That upon identification of this image he followed standard procedure by (A) terminating the search of the device and (B) informing the case agent so that an expanded, follow-up warrant could be obtained. See also Exhibit 2 (HSI report pertaining to initial forensic exam).

## ARGUMENT

Courts in the Sixth Circuit and elsewhere have recognized that the rule of plain view extends to computer searches. See, e.g., United States v. Richards, 659 F.3d 527, 540 (6th Cir. 2011) ("In other words, in general, so long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computers' hard drive in order to determine whether they contain such evidence.") (Citations and internal quotations omitted); United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010) ("Undoubtedly, the warrant's description serves as a limitation on what files may reasonably be searched. The problem with applying this principle to computer searches lies in the fact that such images could be nearly anywhere on the computers. Unlike a physical search object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents").

Courts have also recognized that the limitations of forensic tools and the standard practice of the examiners who use them are both relevant to a plain view inquiry. See, e.g., United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010) ("First, as to the use of the filtering software itself, Detective Huff used it to index and catalogue the files into a viewable format.").

With respect to the discovery of child pornography in plain view during searches for unrelated evidence, it has routinely been held that no suppression is necessary, so long as (1) review ceases upon the discovery and (2) a follow-up warrant is obtained for further searches. See, e.g., United States v. Lucas, 640 F.3d 168, 179-80 (6th Cir. 2011); United States v. Koch, 625 F.3d 470, 478 (8th Cir. 2010); United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001) ("Agent McFarland showed restraint by returning to the magistrate for a new warrant before commencing a new search for evidence of child pornography").[1] This procedure has been institutionalized within the community of law-enforcement forensic examiners, as reflected by the facts described *supra*.

The facts of this case are wholly in accord with both the existing case law and the corresponding best practice of forensic examiners. The examiner had every right pursuant to the original warrant to search image files for evidence relevant to the

[1] Indeed, Courts have even held that the Fourth Amendment is not violated even if the search pursuant to the original warrant continues and more child pornography is uncovered. E.g., Mann, 592 F.3d at 786; United States v. Wong, 334 F.3d 831, 835-38 (9th Cir. 2003).

investigation into violations of 18 U.S.C. 1960, and his tools and methodology for doing so were in accord with both standard practice and technological limitations. When child pornography was discovered and the nature of the case thereby transformed, he ceased his examination and a follow-up warrant was obtained. Exhibits 2 and 3. Suppression, therefore, is not warranted.

Even if the Court were to find that the either the original warrant or the search practices used by the examiner were constitutionally infirm, the fruits of the warrant would survive an analysis under the good faith doctrine. The forensic examiner was conducting and review pursuant to a valid warrant and in accord with standard procedure based on established law. Any violation of law was therefore neither "sufficiently deliberate that exclusion could meaningfully deter it" nor "sufficiently culpable that such deterrence is worth the price paid by the justice system." United States v. Master, 614 F.3d 236, 243 (6th Cir. 2010) (quoting Herring v. United States, 129 S. Ct. 695, 702 (2009).

## CONCLUSION

For the reasons outlined above, the Court should deny STETKIW'S motion to suppress. The Government does not believe an evidentiary hearing is necessary, as the Government believes that the facts are not in dispute.

Respectfully submitted,

MATTHEW SCHNEIDER
United States Attorney

*/s/ TIMOTHY J. WYSE*
Timothy J. Wyse
Assistant U.S. Attorney
(313) 226-9144
211 West Fort, Suite 2001
Detroit, Michigan 48226
Timothy.Wyse@usdoj.gov

December 7, 2018